

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF THE CLAIMS:

1-6. (Canceled)

7. (Currently Amended) [[In]] A trusted element for use with a computer system including an insecure arrangement for using an application ~~and a trusted element for verifying the application, a,~~ the trusted element comprising:

a decryptor that decrypts a credential associated with the application;

a validator that validates at least one digital signature corresponding to the credential;

a challenge generator that selects, based at least in part on the credential, at least one predetermined portion of the application, the predetermined portion of the application including at least some code, and issues a challenge requesting a response from the insecure arrangement, the response providing a computation of at least one value based on the selected predetermined portion of the application; and

a response checker that checks the response against the credential, and determines whether the predetermined portion of the application has been modified.

8. (Original) A trusted element as in claim 7, wherein the challenge generator randomly selects the predetermined portion from plural predetermined portions defined by the credential.

9. (Currently Amended) A trusted element as in claim 7, wherein the challenge generator issues the challenge during execution of the application by the insecure arrangement ~~environment~~.

10. (Original) A trusted element as in claim 7, wherein the challenge generator issues the challenge to the application to compute the value.

11. (Original) A trusted element as in claim 7, wherein the challenge generator requests the application to compute a cryptographic hash of the selected portion.

12. (Original) A trusted element as in claim 7, wherein the challenge generator selects a virtual path within the application.

13. (Original) A trusted element as in claim 7, wherein the challenge generator selects a byte range within the application.

14-27. (Canceled)

28. (New) In an electronic appliance including a secure execution space and an insecure execution space, a method for permitting an application executing within the insecure execution space to request one or more services from a trusted element executing in the secure execution space, the method comprising:

(a) issuing a challenge from the trusted element to the application or an agent of the application, the challenge being based at least in part on randomly selected parts of an authenticated credential, the challenge requesting the application or agent to provide one or more cryptographic hashes of one or more portions of the application;

(b) sending, from the application or agent to the trusted element, said one or more cryptographic hashes of one or more portions of the application;

(c) comparing, at the trusted element, information provided by the authenticated credential with said one or more cryptographic hashes of one or more portions of the application;

(d) denying the application access to said one or more services if the comparison fails.

29. (New) A method as in claim 28, in which steps (a)-(d) are performed multiple times during execution of the application.

30. (New) A method as in claim 28, in which the authenticated credential is digitally signed.

31. (New) A method as in claim 28, in which the authenticated credential is at least in part encrypted.

32. (New) A method as in claim 28, in which the one or more portions of the application include code.

33. (New) A method as in claim 28, in which at least one of the portions of the application overlaps another of the portions of the application.

34. (New) A method as in claim 28, in which at least one of the one or more portions of the application corresponds to a predetermined byte range or virtual path in the application.

35. (New) A computer readable medium storing a computer program, the computer program including instructions that, when executed by a processor of an electronic appliance, are operable to cause the electronic appliance to take actions comprising:

(a) issuing a challenge from a trusted element executing in a secure execution space to an application or agent executing in an insecure execution space, the challenge being based at least in part on randomly selected parts of an authenticated credential, the challenge requesting the application or agent to provide one or more cryptographic hashes of one or more portions of the application;

(b) receiving, from the application or agent, said one or more cryptographic hashes of one or more portions of the application;

(c) comparing information provided by the authenticated credential with said one or more cryptographic hashes of one or more portions of the application;

(d) denying the application access to one or more services provided by an application executing in the secure execution space if the comparison fails.

36. (New) A computer readable medium as in claim 35, in which the computer program is operable to cause the electronic appliance to perform actions (a)-(d) multiple times during execution of the application.

37. (New) A computer readable medium as in claim 35, in which the authenticated credential is digitally signed.

38. (New) A computer readable medium as in claim 35, in which the authenticated credential is at least in part encrypted.

39. (New) A computer readable medium as in claim 35, in which the one or more portions of the application include code.

40. (New) A computer readable medium as in claim 35, in which at least one of the portions of the application overlaps another of the portions of the application.

41. (New) A computer readable medium as in claim 35, in which at least one of the one or more portions of the application corresponds to a predetermined byte range or virtual path in the application.

42. (New) An electronic appliance comprising:
a secure execution space;
an insecure execution space;
a trusted element operable to execute within the secure execution space, the trusted element being operable to:

(a) issue a challenge to an application or agent executing in the insecure execution space, the challenge being based at least in part on randomly selected parts of an authenticated credential, the challenge requesting the application or agent to provide one or more cryptographic hashes of one or more portions of the application;

(b) receive, from the application or agent, said one or more cryptographic hashes of one or more portions of the application;

(c) compare information provided by the authenticated credential with said one or more cryptographic hashes of one or more portions of the application;

(d) deny the application access to one or more services provided by an application executing in the secure execution space if the comparison fails.

43. (New) An electronic appliance as in claim 42, in which the secure execution space comprises a protected processing environment.

44. (New) An electronic appliance as in claim 42, in which the authenticated credential is digitally signed and at least in part encrypted.

45. (New) An electronic appliance as in claim 42, in which the one or more portions of the application include code.

46. (New) An electronic appliance as in claim 45, in which at least one of the portions of the application overlaps another of the portions of the application.

47. (New) An electronic appliance as in claim 46, in which at least one of the one or more portions of the application corresponds to a predetermined byte range or virtual path in the application.